

Exhibit A

Rebecca Davis (SBN 271662)
rebecca@lozeaudrury.com
LOZEAU DRURY LLP
1939 Harrison St., Suite 150
Oakland, CA 94612
Telephone: (510) 836-4200
Facsimile: (510) 836-4205

Patrick H. Peluso*
ppeluso@woodrowpeluso.com
Steven L. Woodrow*
swoodrow@woodrowpeluso.com
WOODROW & PELUSO, LLC
3900 East Mexico Avenue, Suite 300
Denver, Colorado 80210
Telephone: (720) 213-0675
Facsimile: (303) 927-0809

**Pro Hac Vice* admission to be sought

Attorneys for Plaintiff and the Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

Loretta Williams, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

**What If Holdings, LLC d/b/a C4R Media
Corp., and ActiveProspect, Inc.**

Defendants.

Case No. 3:22-cv-03780-WHA

**[PROPOSED] FIRST AMENDED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMANDED

1. Plaintiff Loretta Williams (“Plaintiff” or “Williams”) brings this Class Action Complaint and Jury Demand (“Complaint”) against Defendants What If Holdings, LLC d/b/a C4R Media Corp. (“C4R Media”) and ActiveProspect, Inc. (“ActiveProspect”) to obtain redress for, and to put an end to, Defendants’ serial wiretapping of the electronic communications of visitors to C4R Media’s websites, including claim.foundmoneyguide.com.

2. The wiretaps are embedded in the computer code on C4R Media’s websites and are used by Defendants to covertly observe and record visitors’ keystrokes and clicks in real time.

1 and clicks. It plays these events back as a screen capture of how the user interacted with the page.”
 2 See “Certificate of Authenticity for Web Leads,” attached hereto as Exhibit A.

3 9. In 2020, ActiveProspect’s CEO Steve Rafferty appeared as a guest on a TCPA-
 4 related podcast called “Unprecedented,” in which he and the CEO of Jornaya, a competing lead
 5 verification company, discussed their businesses.¹ The podcast hosts introduced the companies as
 6 “the guardian angels of the TCPAWorld, keeping watch over millions of website interactions each
 7 month.” During the interview, Rafferty repeatedly referred to the ActiveProspect as an
 8 “independent third party” who “monitors” activity on a given lead website—Rafferty described
 9 ActiveProspect as “there as an independent third party [who can] say, ‘hey this is what really
 10 happened.’ You don’t have to trust the buyer or the seller of the lead, you can trust
 11 [ActiveProspect]. We were there. Here is what happened.” Rafferty further explained that
 12 ActiveProspect “can send [information] directly” to other parties that request it.

13 10. ActiveProspect’s involvement in the recording process is not merely that of a
 14 device, but a third party. As described in the abstract of its patent, ActiveProspect operates a
 15 “verification server” that collects, processes, aggregates, stores, and ultimately produces recordings
 16 of website visits upon request:

17 A lead generator contacts a verification server [*i.e.*, ActiveProspect] when a
 18 visitor lands on a hosting site of the lead generator to enter lead information into a
 19 form. **The verification server issues a reference key (token) to the lead**
 20 **generator and collects information about the visitor and the hosting site of the**
 21 **lead generator, using the reference key to identify the collected information.**
 22 When the visitor submits the form, the lead generator sends the form data, which
 23 includes the entered lead information and the reference key received from the
 24 verification server, to at least one interested party. **When the verification server**
receives a request for the collected information from the interested party, the
collected information is retrieved based on the reference key included in the
request and sent to the requesting interested party.

25 U.S. Patent No. 2012/0290491 A1, at (57) (filed May 12, 2011) (emphasis added) (attached hereto
 26

27 ¹ *Unprecedented Episode 19*, TCPAWorld, [https://players.brightcove.net/5807743129001/](https://players.brightcove.net/5807743129001/default_default/index.html?videoId=6217015344001)
 28 [default_default/index.html?videoId=6217015344001](https://players.brightcove.net/5807743129001/default_default/index.html?videoId=6217015344001).

1 as Exhibit B).

2 11. The patent likewise states that “the verification server collects information about the
3 visitor and the lead generator during the communication session during which the lead generator
4 receives contact information and other relevant information (i.e. lead data) submitted by the
5 visitor.” (Ex. B at [0027].) The patent further explains that the script embedded in a lead
6 generator’s website “provides to the verification server [*i.e.*, ActiveProspect] the URL of the web
7 page where the form resides. At this point, **the verification server is “aware” of the URL of the**
8 **form and begins to monitor the web page** for any changes.” (*Id.* at [0057]) (emphasis added).

9 12. In addition to being intrusive, technology like TrustedForm poses a threat to
10 consumer security. In a 2017 study, Princeton University researchers noted that “[c]ollection of
11 page content by third-arty replay scripts may cause sensitive information such as medical
12 conditions, credit card details, and other personal information displayed on a page to leak to the
13 third-party as part of the recording. This may expose users to identify theft, online scams, and other
14 unwanted behavior.”² The study found that “the extent of data collected by these services far
15 exceeds user expectations; text typed into forms is collected **before the user submits the form,**
16 **and precise mouse movements are saved, all without any visual indication to the user.”**
17 (emphasis added).

18 13. ActiveProspect enters into partnerships with various telemarketers and lead
19 generators who wish to utilize TrustedForm. ActiveProspect provides its software and scripts to
20 those partners, and ActiveProspect thereafter is enabled to record visits to the partners’ websites.

21 14. One such entity is C4R Media, which used TrustedForm to record visitors to its
22 website claim.foundmoneyguide.com and other websites that it operates.

23 15. C4R Media knows that TrustedForm captures strokes, clicks, and other interactions
24 on its websites—it is a primary reason why C4R Media contracts with ActiveProspect for the
25 TrustedForm product in the first place.

26
27 ² Michael Kassner, *Session-replay scripts disrupt online privacy in a big way*, TECHREPUBLIC
28 (Dec. 26, 2017), <https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/>

the events and omissions giving rise to the claims occurred in this District.

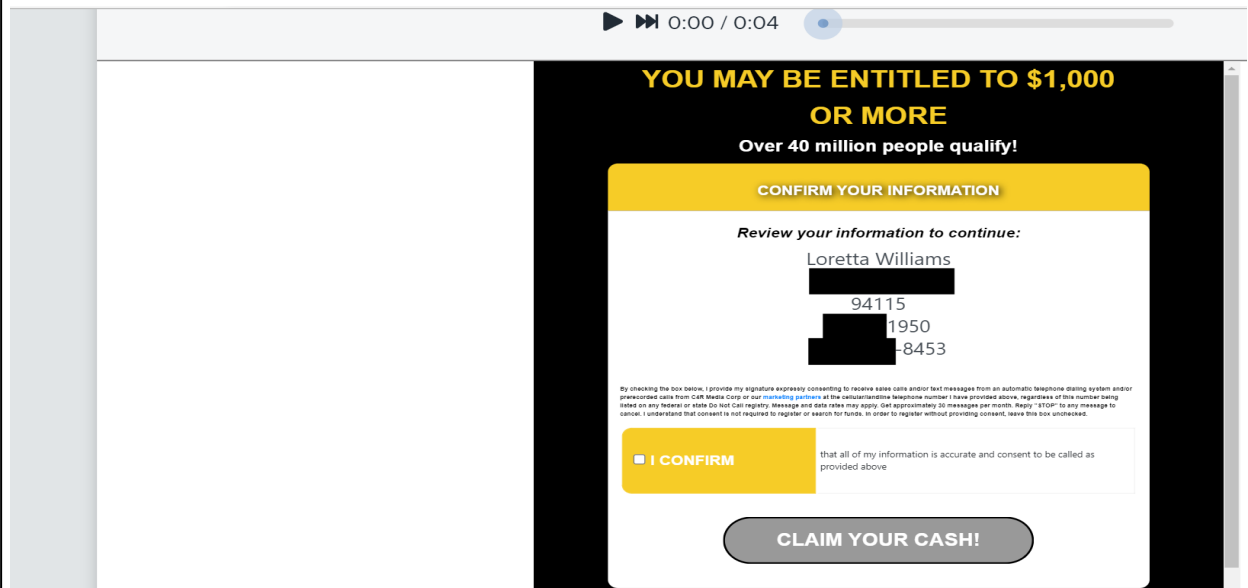
FACTS SPECIFIC TO PLAINTIFF

25. On or around December 24, 2021, Williams visited claim.foundmoneyguide.com/api/offer, a website owned and operated by C4R Media.

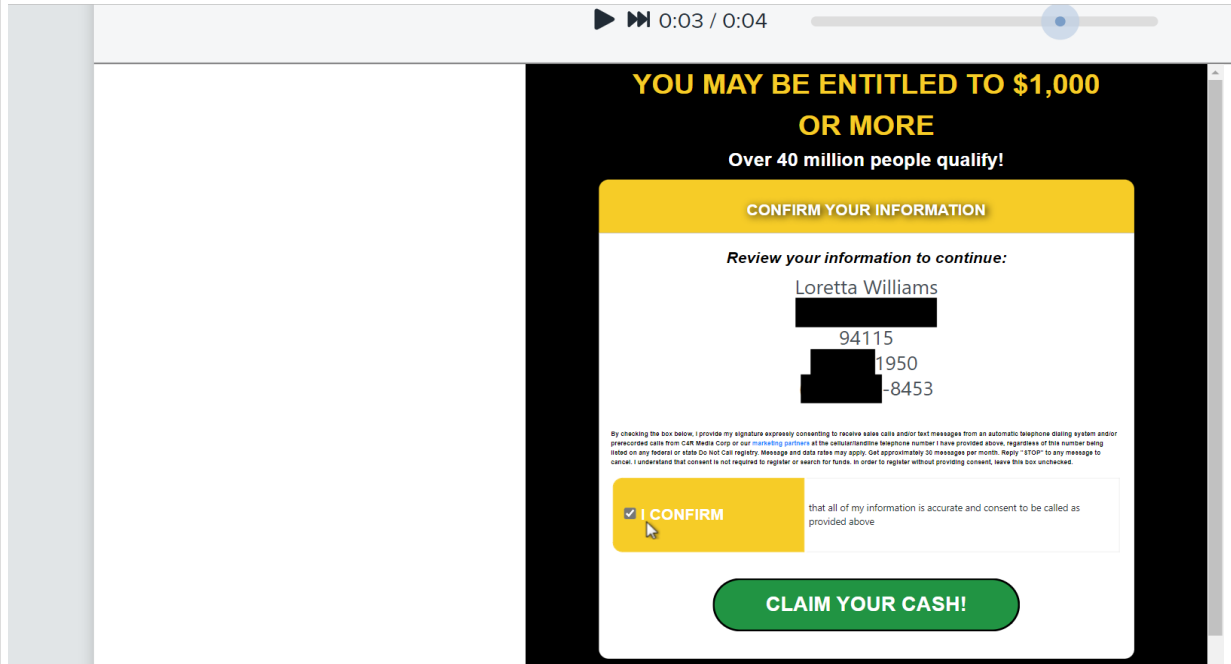
26. During that visit, Defendants recorded her visit through the use of ActiveProspect's TrustedForm replay function. The video captured Williams' keystrokes and clicks on the website, as well as the date and time of her visit, the browser and operating system used by Williams during the visit, and her geographic location.

27. TrustedForm also recorded Williams' name, address, date of birth, and phone number.

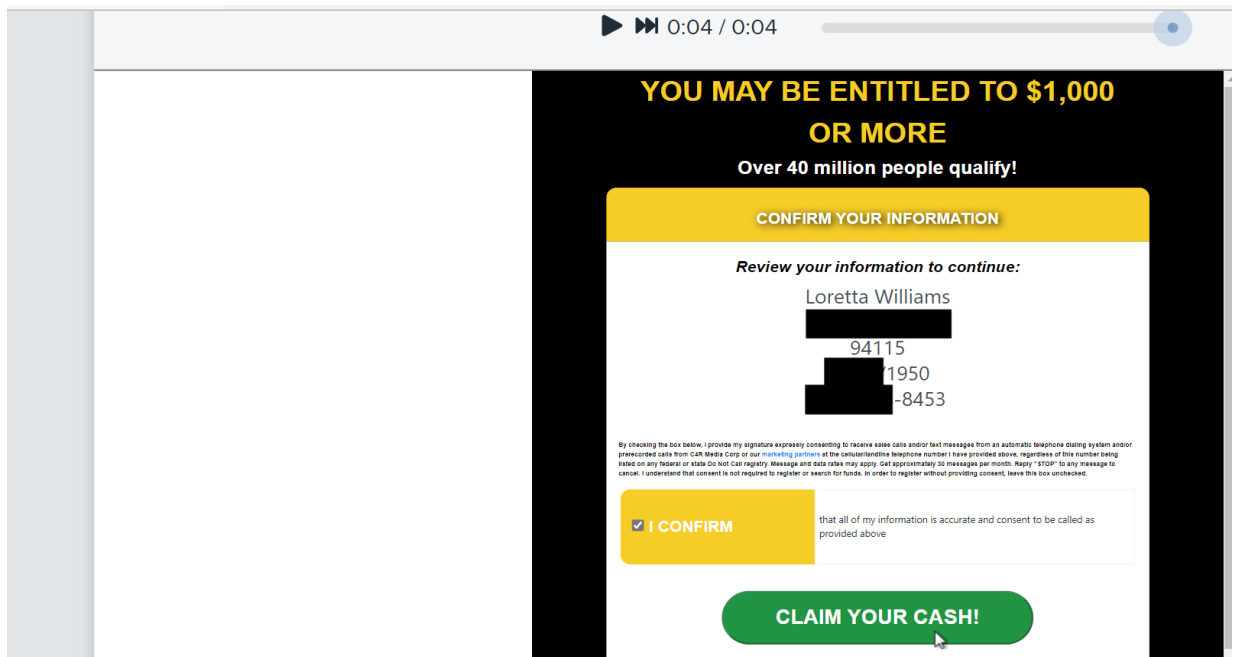
28. A screenshot of the TrustedForm recording related to Williams's visit is below:



29. As the screenshot of the TrustedForm replay shows, Williams' personal information is included on the page. But at this point in the video, the "I CONFIRM" button is not clicked. However, approximately 3 seconds into the video, Williams' cursor appears and clicks "I CONFIRM":



30. Then one additional second later, the cursor moves over to the green "CLAIM YOUR CASH!" button:



31. Thus, Williams' interaction (including her keystrokes and mouse movement and

**FIRST AMENDEND
CLASS ACTION COMPLAINT**

clicks) was recorded by C4R Media and ActiveProspect using ActiveProspect's TrustedForm technology.

32. This recording was done without Plaintiff's consent. Defendants did not inform website visitors that their strokes and clicks would be recorded, much less secure prior express consent. Indeed, the wiretapping began the moment Williams and other members of the alleged Class visited the webpage, before clicking any button.

33. All TrustedForm videos are hosted on ActiveProspect's servers, not the servers of website clients like C4R Media. In order to access the videos, an interested party must make a request to and follow a unique URL hyperlink provided by ActiveProspect associated with the recording on its server. Moreover, ActiveProspect independently collects and stores information provided by web users on the websites of its clients.

34. Members of the alleged Class were unlawfully monitored in the same way as Williams' was: TrustedForm functions the exact same way no matter which persons is visiting a site, or which of C4R's websites the person is visiting.

35. For wiretapping her visit to C4R's visit, Plaintiff brings this suit, on behalf of herself and those similarly situated, to put an end to Defendants' repeated and widespread CIPA violations. Such violations entitle her, and other similarly situated persons, to injunctive relief plus statutory damages of \$5,000 per violation.

CLASS ACTION ALLEGATIONS

36. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure Rules 23(b)(2) and 23(b)(3) on behalf of herself and a Class defined as follows:

All persons in California who: (1) from a date one year prior to the filing of the initial complaint in this action to the date notice is sent to the Class; (2) visited one of C4R Media's websites; (3) which utilized ActiveProspect's "TrustedForm" software; (4) who had their electronic communications intercepted and/or recorded by ActiveProspect; and (5) where the Defendants claim to have secured prior express consent to monitor, record, collect, and store electronic communications in the same manner as they claim to have secured prior express consent from Williams, or where Defendants do not claim they secured any such prior express consent.

37. Excluded from the Class are: (1) Defendants, Defendants' agents, subsidiaries,

1 parents, successors, predecessors, and any entity in which Defendants or their parents have a
 2 controlling interest, and those entities' officers and directors, (2) the Judge or Magistrate Judge to
 3 whom this case is assigned and the Judge's or Magistrate Judge's immediate family, (3) Plaintiff's
 4 counsel and Defendants' counsel; (4) persons who execute and file a timely request for exclusion,
 5 (5) persons who have had their claims in this matter finally adjudicated and/or otherwise released,
 6 and (6) the legal representatives, successors, and assigns of any such excluded person. Plaintiff
 7 anticipates the need to amend the class definition following a reasonable period for discovery
 8 regarding the contours of the Class.

9 38. **Numerosity:** The exact number of class members is unknown to Plaintiff at this
 10 time, but it is clear that individual joinder is impracticable. On information and belief, Defendants
 11 wiretapped thousands of California residents. Further, the class members can readily be ascertained
 12 through Defendants' records.

13 39. **Commonality:** Common questions of law and fact exist as to all members of the
 14 Class for which this proceeding will provide common answers in a single stroke based upon
 15 common evidence, including:

- 16 (a) Whether Defendants' conduct described herein violated the CIPA;
- 17 (b) Whether Defendants secured prior express consent before monitoring, recording,
 18 collecting, and storing the electronic communications of Plaintiff and the Class;
- 19 (c) Whether Defendants have violated the California Constitution; and
- 20 (d) The proper measure of damages.

21 40. **Typicality:** As a result of Defendants' uniform and repeated pattern of unlawful
 22 recording, Plaintiff and the class members suffered the same injury and similar damages. If
 23 Defendants' actions violated the CIPA as to Plaintiff, then they violated the CIPA as to all class
 24 members. Thus, Plaintiff's claims are typical of the claims of the other class members.

25 41. **Adequate Representation:** Plaintiff is a member of the Class and both she and her
 26 counsel will fairly and adequately represent and protect the interests of the Class, as neither has
 27 interests adverse to those of the class members and Defendants have no defenses unique to
 28 Plaintiff. In addition, Plaintiff has retained counsel competent and experienced in complex

litigation and class actions. Further, Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the financial resources to do so.

42. **Conduct Applicable Towards Class as a Whole:** Defendants acted consistently with respect to every member of the Class. No Class Member was treated specially or different as Defendants acted in the same manner with respect to all Class Members. As such, injunctive relief and corresponding declaratory relief are available and appropriate.

43. **Predominance:** The common questions of law and fact set forth above go to the very heart of the controversy and predominate over any supposed individualized questions. Irrespective of any given class member's situation, the answer to whether Defendants' conduct described herein repeatedly violated the CIPA is the same for everyone—a resounding “yes”—and the same will be proven using common evidence.

44. **Superiority and Manageability:** A class action is superior to all other methods of adjudicating the controversy. Joinder of all class members is impractical, and the damages suffered by/available to the individual class members will likely be small relative to the cost associated with prosecuting an action. Thus, the expense of litigating an individual action will likely prohibit the class members from obtaining effective relief for Defendants' misconduct. In addition, there are numerous common factual and legal questions that could result in inconsistent verdicts should there be several successive trials. In contrast, a class action will present far fewer management difficulties, as it will increase efficiency and decrease expense. Further, class-wide adjudication will also ensure a uniform decision for the class members.

FIRST CAUSE OF ACTION
Violation of Cal. Penal Code § 631, *et seq.*
(On Behalf of Plaintiff and the Class)

45. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

46. The CIPA provides that it is a violation of Cal. Penal Code § 631(a) for a defendant, “by means of any machine, instrument, contrivance, or in any other matter,” to do any of the following:

Intentionally tap[], or make[] any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, read[] or attempt[] to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

Or

Use[], or attempt[] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

Or

Aid[], agree[] with, employ[], or conspire[] with any person or persons to unlawfully do, or permit or cause to be done any of the acts or things mentioned above in this section.

47. Section 631(a) is not limited to phone lines. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc. Internet Tracking Litigation*, --- F.3d --- 2020 WL 1807978 (9th Cir. Apr. 9, 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook’s collection of consumers’ Internet browsing history).

48. TrustedForm is a “machine, instrument, contrivance, or . . . any other manner” that is used by ActiveProspect and C4R Media to engage in the unlawful practices described in this Complaint.

49. By using TrustedForm, Defendants intentionally tapped the lines of communication between Plaintiff (and absent Class Members) and C4R Media’s websites by willfully and without consent reading or attempting to read or learn the contents or meaning of electronic

1 communications of Plaintiff and the putative class members, while such communications were in
2 transit or passing over any wire, line or cable or were being sent from or received at any place
3 within California.

4 50. Defendants lack prior express consent from Plaintiff and the Class for Defendants to
5 “read or attempt to read or learn the contents or meaning” of their electronic communications being
6 made in the State of California.

7 51. C4R Media partnered with (and conspired with) ActiveProspect to achieve the
8 unlawful conduct described herein.

9 52. This violation of Section 631(a) is an invasion of privacy and confers Article III
10 standing.

11 53. Absent an injunction, Plaintiff and the members of the Alleged Class are at risk of
12 continued harm. TrustedForm is used by many website operators and there is no practical way to
13 know if the future whether website communications will be monitored and recorded by
14 Defendants, absent ceasing to utilize the internet (a near impossibility in the year 2022).

15 54. Accordingly, pursuant to Cal. Penal Code § 637.2(a)(1), Plaintiff and the Class seek
16 injunctive relief and statutory damages in the amount of \$5,000 per violation.

17 **SECOND CAUSE OF ACTION**
18 **Invasion of Privacy Under California’s Constitution**
19 **(On Behalf of Plaintiff and the Class)**

20 55. Plaintiff incorporates by reference the foregoing allegations as if fully set forth
21 herein.

22 56. Plaintiff and other members of the Class have an interest in conducting personal
23 activities (such as visiting websites), without observation or interference, including visiting
24 websites without being subjected to secret wiretaps.

25 57. Defendants intentionally invaded the privacy rights of Plaintiff and other members
26 of the Class, and worked cooperatively to do so.

27 58. This invasion of privacy is serious in nature and scope and constitutes a breach of
28 the social norms in the digital age.

59. Thus, Plaintiff seeks all relief available for invasion of privacy under the California Constitution on behalf of herself and members of the alleged Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that this Court issue an order:

- A. Certifying this case as a class action on behalf of the Class defined above, appointing Williams as class representative and appointing her counsel as class counsel;
- B. Finding that Defendants' actions constitute repeated and willful violations of the CIPA;
- C. Awarding injunctive relief under the CIPA enjoining Defendants from continuing to violate the CIPA by unlawfully wiretapping electronic communication without consent;
- D. Awarding damages, including statutory damages where applicable, to Plaintiff and the Class in amounts to be determined at trial;
- E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;
- F. Awarding Plaintiff and the Class pre- and post- judgment interest, to the extent allowable; and
- G. Such further and other relief as the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully submitted,

Dated: January 5, 2023

LORETTA WILLIAMS, individually and on behalf
of all others similarly situated,

By: /s/ Patrick H. Peluso
One of Plaintiff's Attorneys

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Rebecca Davis (SBN 271662)
rebecca@lozeaudrury.com

LOZEAU DRURY LLP
1939 Harrison St., Suite 150
Oakland, CA 94612
Telephone: (510) 836-4200
Facsimile: (510) 836-4205

Patrick H. Peluso*

ppeluso@woodrowpeluso.com

Steven L. Woodrow*

swoodrow@woodrowpeluso.com

WOODROW & PELUSO, LLC
3900 East Mexico Avenue, Suite 300
Denver, Colorado 80210
Telephone: (720) 213-0675
Facsimile: (303) 927-0809

**Pro Hac Vice*

Counsel for Plaintiff and the Class

Exhibit A

Certificate of Authenticity for Web Leads

✓ Claimed

Certificate

Screen Capture

Event Log

Claim History

Certificate of Authenticity for Web Leads



Certificate ID: e33d56c57352424c07841d4f200e1564dc9848

This certificate was issued by TrustedForm.com from ActiveProspect, the independent Internet lead certification authority. It certifies the following information about this lead:

When did they visit?

Visit date:

December 24, 2021

Visit time:

7:39:12 AM MST

Time on page:

4 seconds

Where did they visit?

Who visited?

Remote IP Address:

73.18 [REDACTED]

Geographic Location (Approximate):

San Francisco, California, United States

Browser:

Safari 15.2

Operating System:

Mac OS X 10.15.6

What did they see?

Trustedform captures a copy of the web page viewed by the visitor and the user events that took place on the page including form inputs, mouse movements and clicks. It plays these events back as a screen capture of how the user interacted with the page.

[View Screen Capture](#)

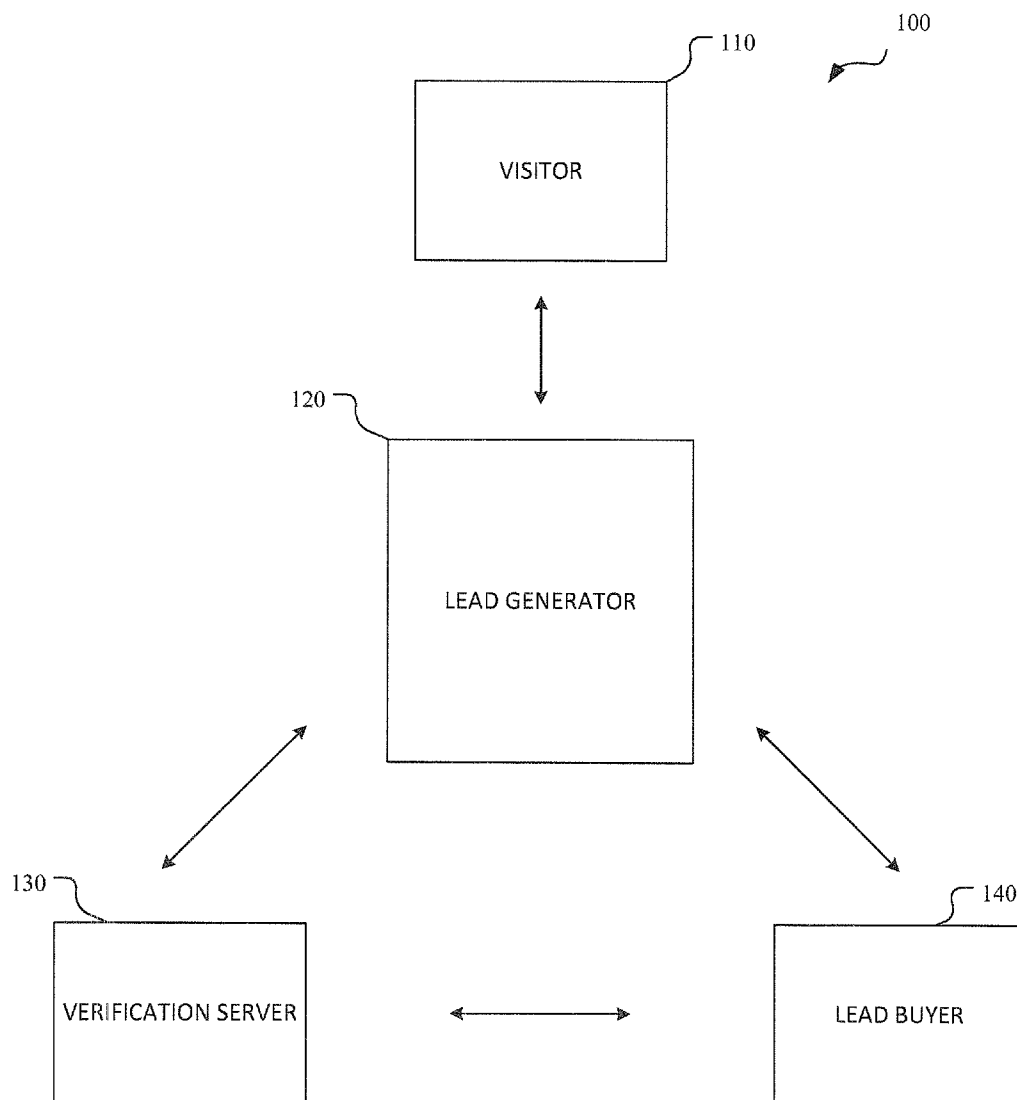
Exhibit B



US 20120290491A1

(19) **United States**(12) **Patent Application Publication**
Rafferty et al.(10) **Pub. No.: US 2012/0290491 A1**(43) **Pub. Date: Nov. 15, 2012**(54) **SYSTEM AND METHOD FOR ELECTRONIC
LEAD VERIFICATION**(52) **U.S. Cl. 705/317**(75) **Inventors:** **Steven M. Rafferty**, Austin, TX
(US); **Rickie N. Benavidez**, Kyle,
TX (US); **Alexander K. Wolfe**,
Austin, TX (US); **Michael Shapiro**,
Hoboken, NJ (US)(57) **ABSTRACT**

A system and a method provide a lead verification service. A lead generator contacts a verification server when a visitor lands on a hosting site of the lead generator to enter lead information into a form. The verification server issues a reference key (token) to the lead generator and collects information about the visitor and the hosting site of the lead generator, using the reference key to identify the collected information. When the visitor submits the form, the lead generator sends the form data, which includes the entered lead information and the reference key received from the verification server, to at least one interested party. When the verification server receives a request for the collected information from the interested party, the collected information is retrieved based on the reference key included in the request and sent to the requesting interested party.

(73) **Assignee:** **ActiveProspect, Inc.**, Austin, TX
(US)(21) **Appl. No.: 13/106,641**(22) **Filed: May 12, 2011****Publication Classification**(51) **Int. Cl.**
G06Q 99/00 (2006.01)

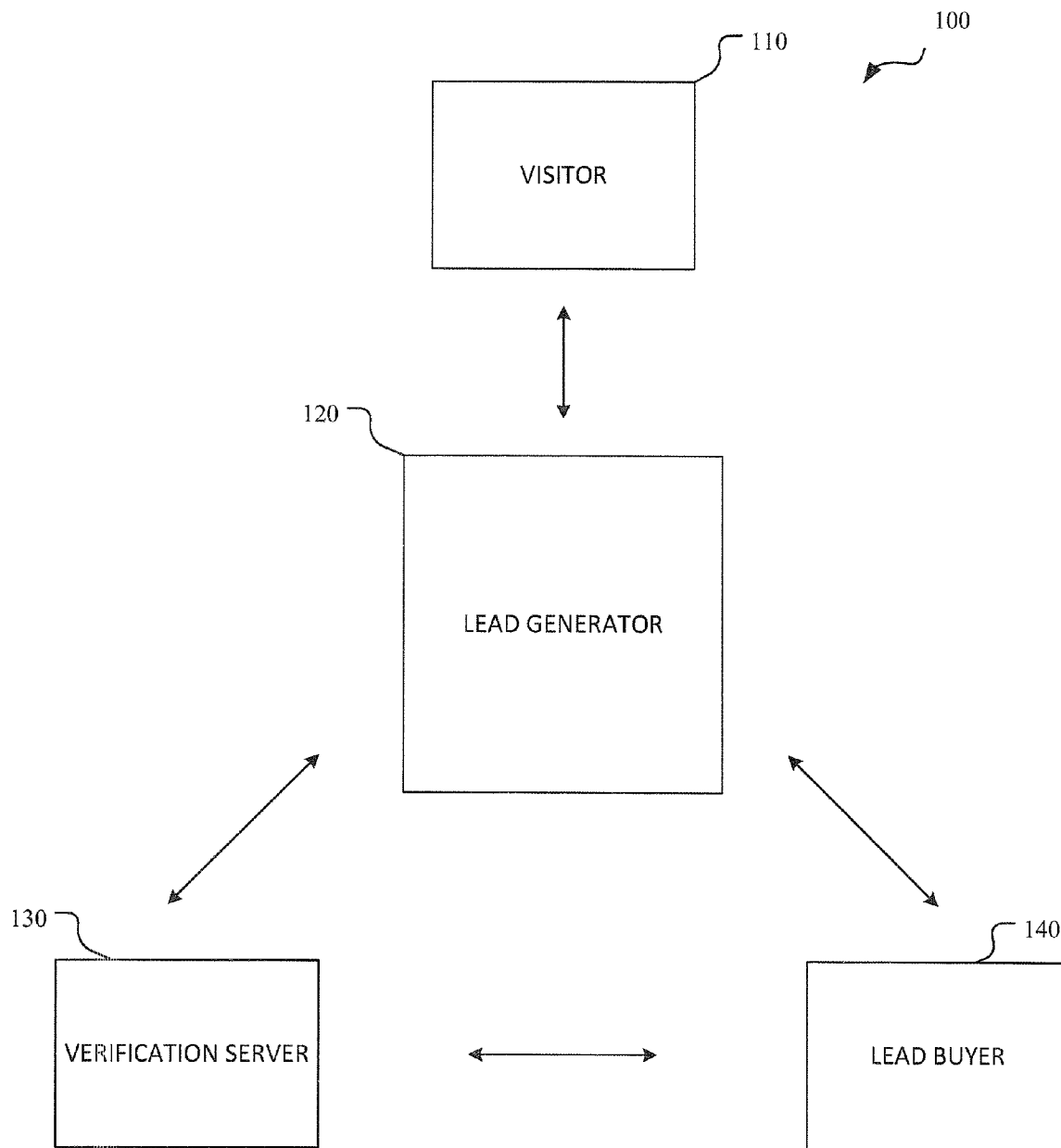


FIGURE 1

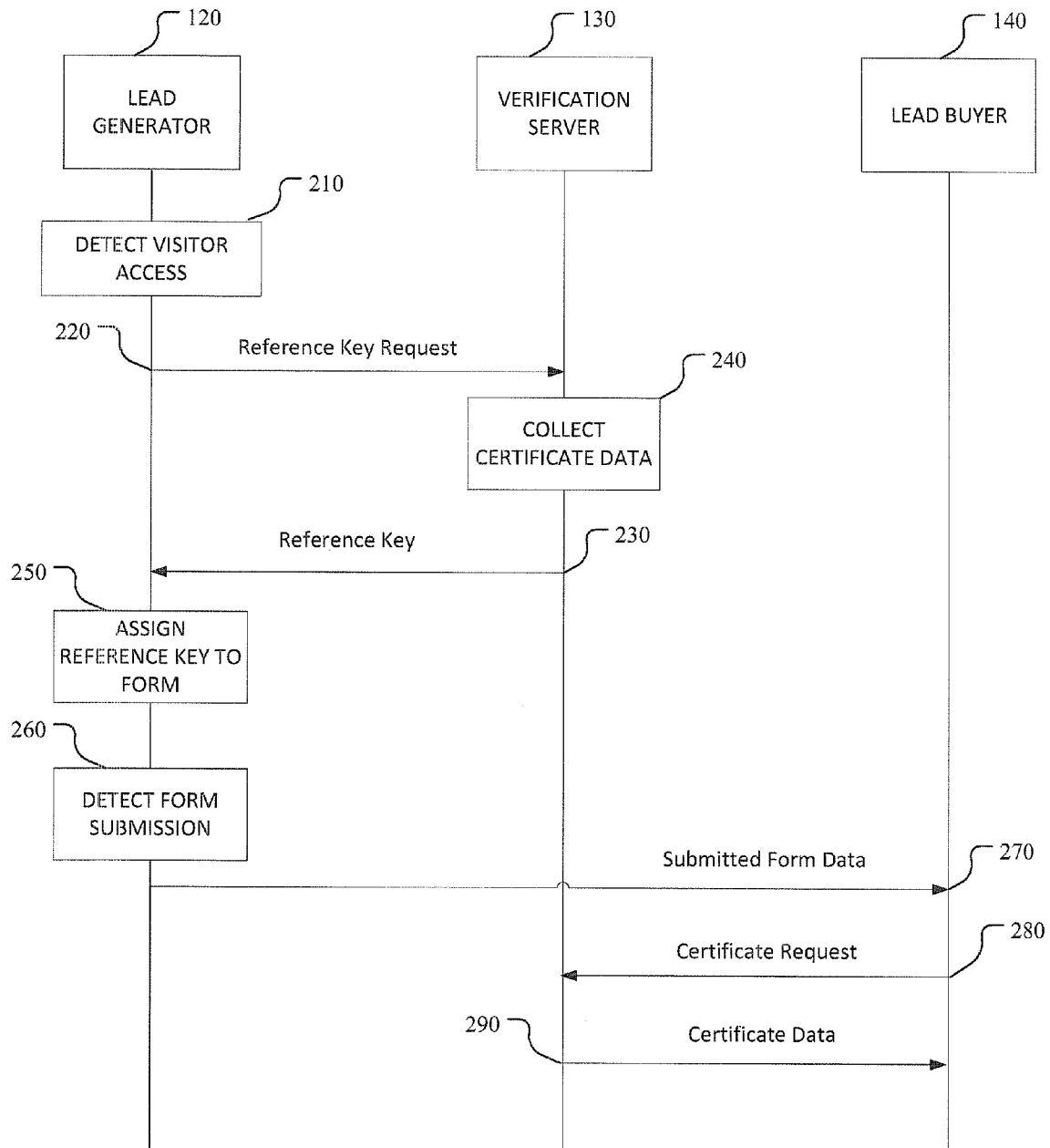


FIGURE 2

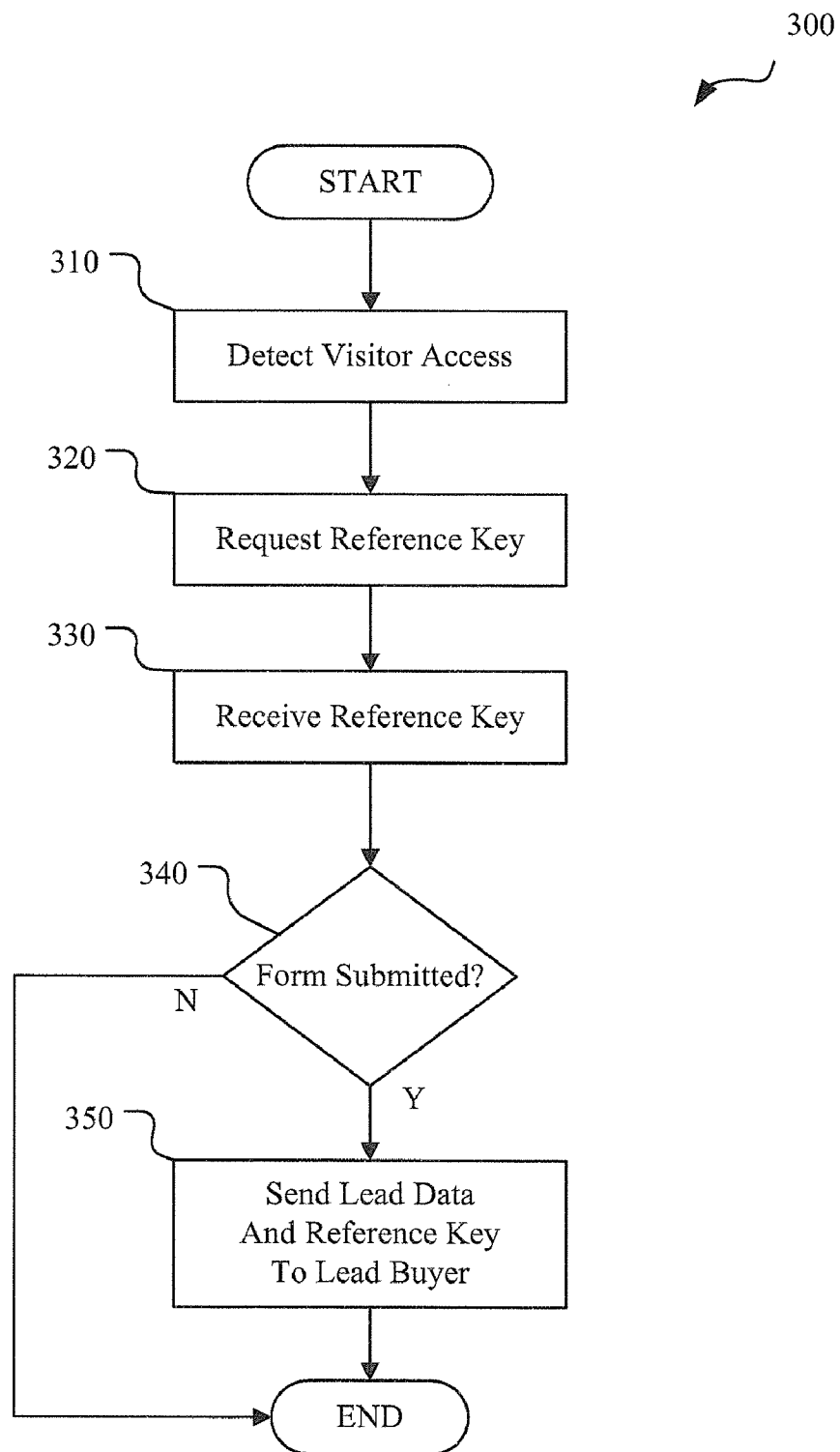


FIGURE 3

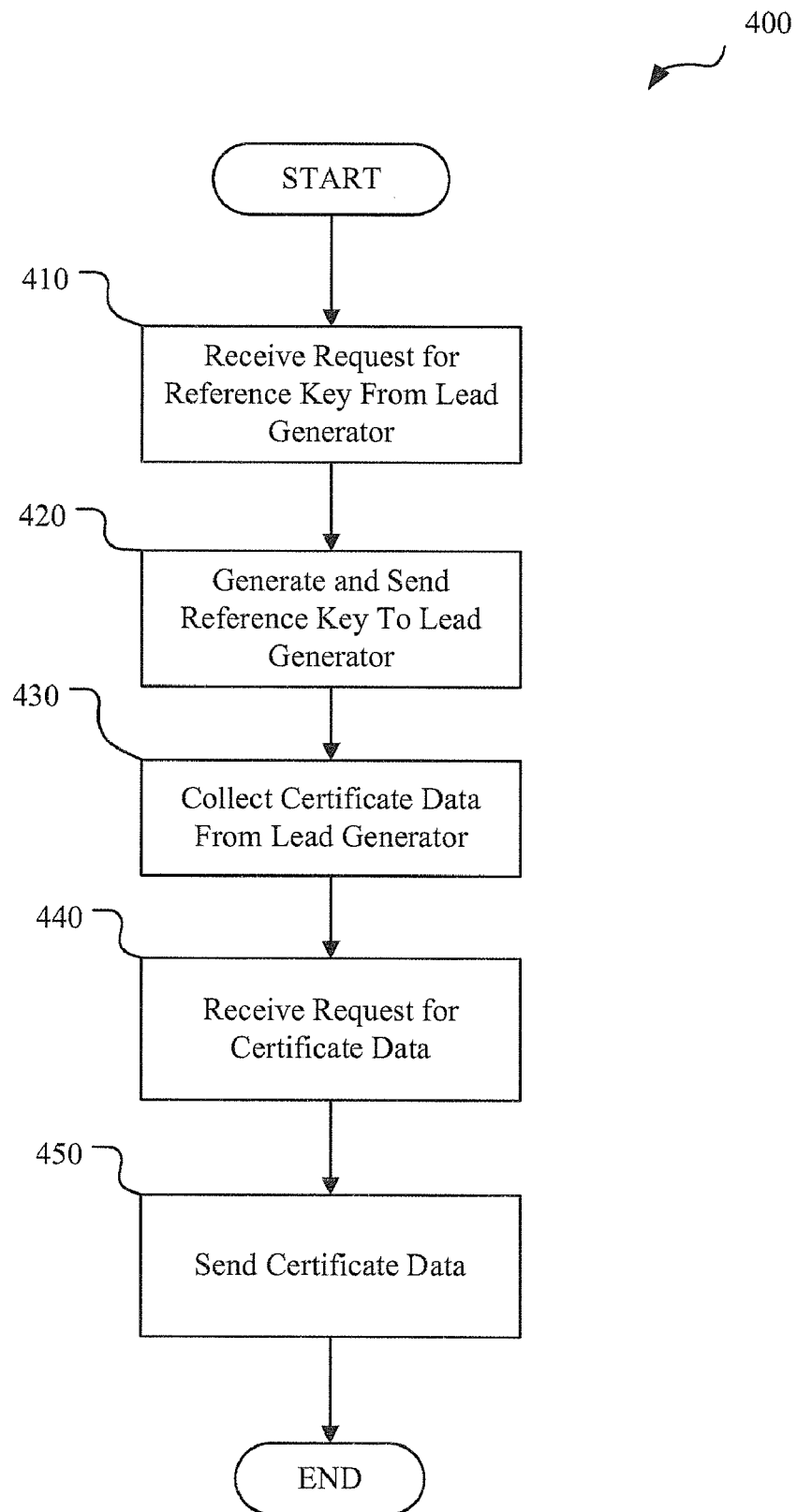


FIGURE 4

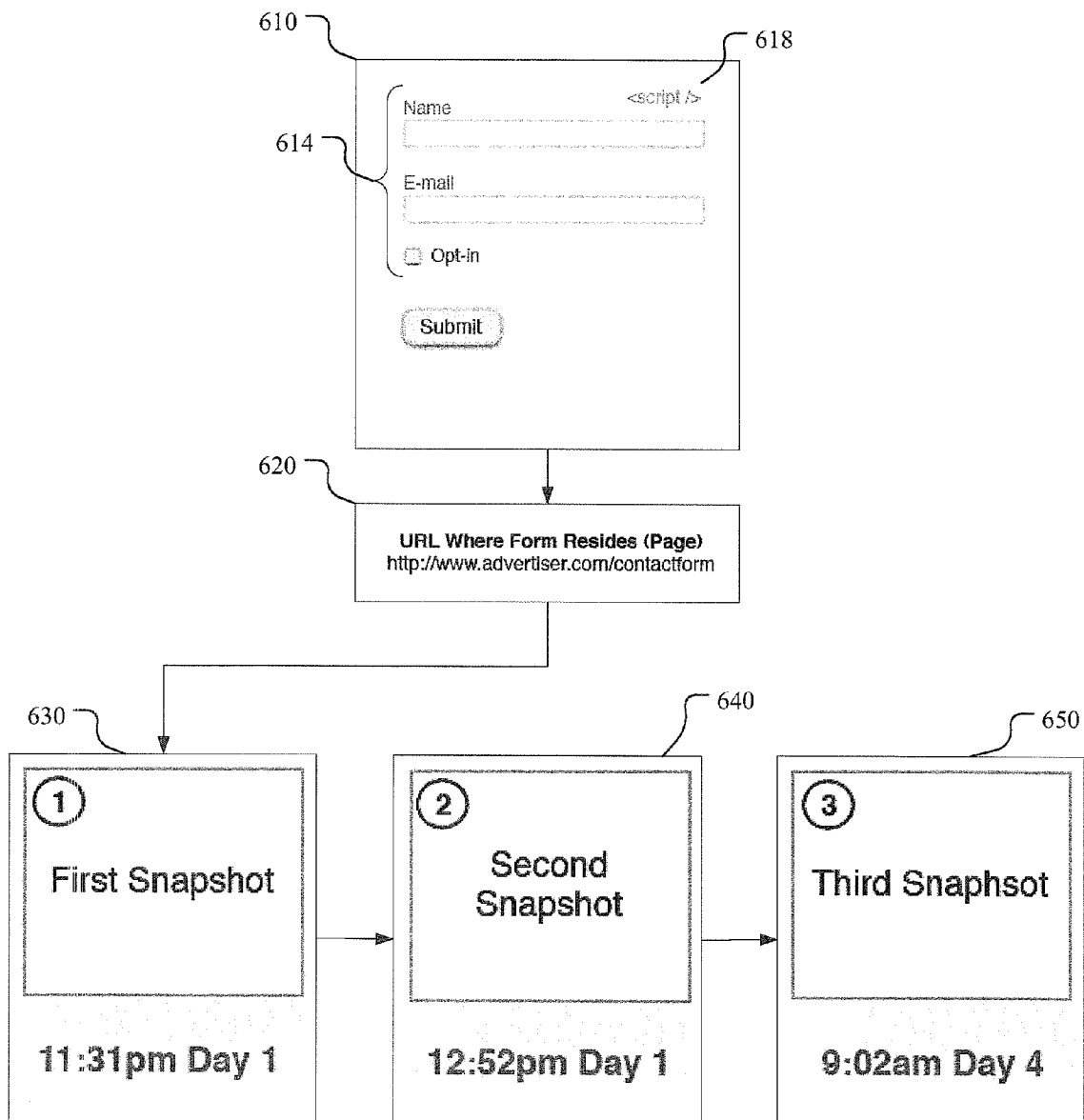


FIGURE 5

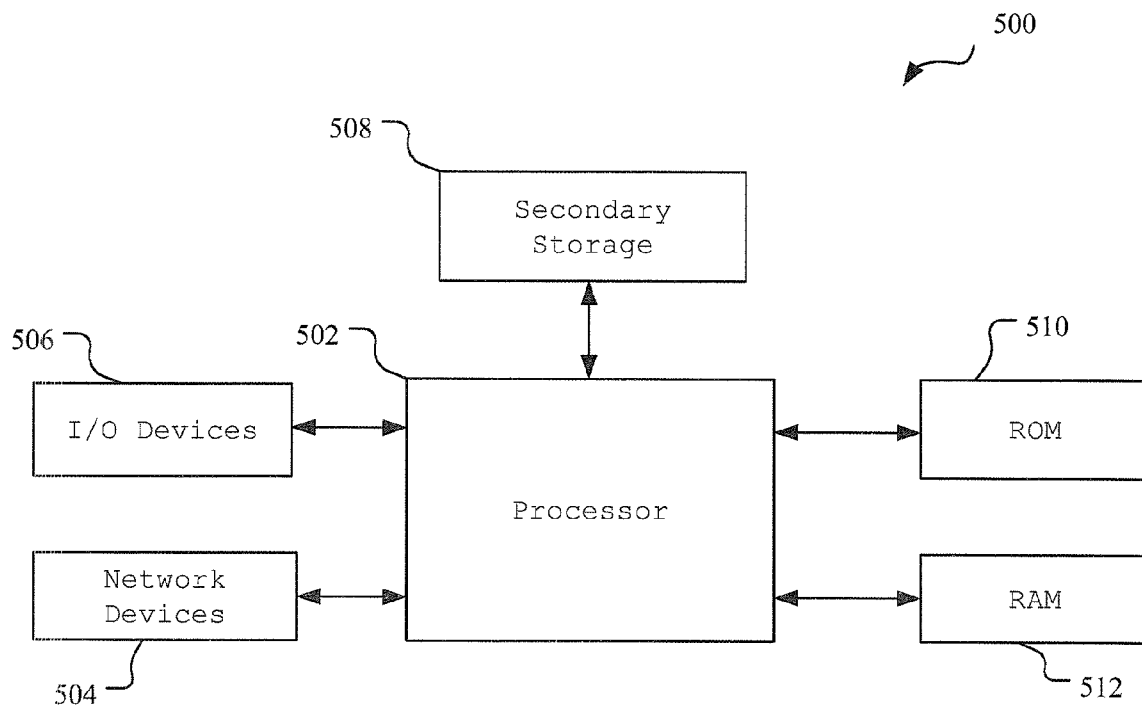


FIGURE 6

US 2012/0290491 A1

Nov. 15, 2012

1

SYSTEM AND METHOD FOR ELECTRONIC LEAD VERIFICATION

TECHNICAL FIELD OF THE INVENTION

[0001] The present disclosure is directed, in general, to communication systems, and more specifically, to a system and method for verifying a lead that was collected from a website.

BACKGROUND OF THE INVENTION

[0002] “Lead generation” generally refers to the creation or generation of prospective consumer interest or inquiry into products or services of a business. There has been a recent trend towards lead generation using the Internet. In a typical lead generation scenario, a consumer completes an online request form on a website. When the form is completed and submitted, the consumer’s information may be sent to a party interested in the data or alternatively evaluated to match the consumer with one or more appropriate providers. Typically, the lead generation website is owned and operated by one party (the lead seller) while a separate party receives the data (the lead buyer).

[0003] Currently, there are no reliable means for a lead buyer to verify when and where an Internet lead was collected by a lead seller. Since the lead seller hosts the web form, the buyer that purchases leads has no control of the form used to collect the lead and therefore may not be able to verify where the lead was collected or if it was even collected on a web form. The lead buyer is unable to verify basic information about the lead and is therefore unable to verify the authenticity of the lead. On what website was it collected? What information was presented to the consumer on the web page? When was it collected? Was it submitted by a consumer from a web browser? What was the IP address of the consumer submitting the lead? To answer these questions the buyer must rely on the word of the seller with no way to independently verify. Because of this basic lack of transparency it is easy for a lead seller to take advantage of a lead buyer by misrepresenting when, where and how leads were collected. For example, a lead seller may represent that the lead was collected on one site when it was in fact collected on another.

[0004] As such, there is a need for an improved means for independently verifying the authenticity of leads that are generated from lead generating websites.

SUMMARY OF THE INVENTION

[0005] According to one aspect of the present invention, a method of providing a verification token (aka certificate of authenticity) with an internet lead is provided. A verification server is notified when a visitor accesses a web page to enter information into a form. A reference key comprising a unique identifier is received from the verification server. And in response to the visitor submitting the form, the form data is sent to at least one interested party. The form data includes the reference key and the information entered by the visitor.

[0006] According to another aspect of the present invention, a method of a verification server for supporting a lead verification service is provided. A reference key that includes a unique identifier is generated in response to receiving a notification from a lead generator on a website that is being accessed by a visitor. The reference key is sent to the lead generator. Information about the lead generator and the visitor that is accessing the website is collected. The collected

information is associated with the reference key. The collected information is sent to at least one interested party in response to receiving a valid request comprising the reference key.

[0007] According to another aspect of the present invention, a system for supporting a lead verification service is provided. The system includes a verification server and a web server that is hosting a website comprising a lead generator. The lead generator is configured to notify the verification server when a visitor accesses the website to enter information into a form, receive a reference key comprising a unique identifier from the verification server, and send the form data to at least one interested party in response to the visitor submitting the form, the form data comprising the reference key and the information entered by the visitor.

[0008] According to yet another embodiment of the present invention, an apparatus for supporting a lead verification service is provided. The apparatus includes a communication interface, a memory, and a processor. The communication interface sends and receives information. The memory stores instructions for providing lead information that can be verified. And the processor performs the instructions stored in the memory to generate a verification token that includes a unique identifier in response to receiving a notification from a lead generator on a website that is being accessed by a visitor, send the verification token to the lead generator, collect information about the lead generator and the visitor that is communicating with the lead generator, and send the collected information to an interested party, in response to receiving a valid request, based on the verification token.

[0009] In some embodiments, the system ensures that the information collected and associated with a particular reference key is valid. When the lead generator communicates with the verification server, there are multiple interactions between the systems (i.e. the verification server and the system on which an instance of the lead generator is being executed) to help ensure that the information collected is accurate and the lead generator is not trying to misrepresent that information.

[0010] Before undertaking the DETAILED DESCRIPTION OF THE INVENTION below, it may be advantageous to set forth definitions of certain words and phrases used throughout this patent document: the terms “include” and “comprise,” as well as derivatives thereof, mean inclusion without limitation; the term “or,” is inclusive, meaning and/or; the phrases “associated with” and “associated therewith,” as well as derivatives thereof, may mean to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, or the like; and the term “controller” means any device, system or part thereof that controls at least one operation, such a device may be implemented in hardware, firmware or software, or some combination of at least two of the same. It should be noted that the functionality associated with any particular controller may be centralized or distributed, whether locally or remotely. Definitions for certain words and phrases are provided throughout this patent document, those of ordinary skill in the art should understand that in many, if not most instances, such definitions apply to prior, as well as future uses of such defined words and phrases.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] For a more complete understanding of the present disclosure and its advantages, reference is now made to the

US 2012/0290491 A1

Nov. 15, 2012

2

following description taken in conjunction with the accompanying drawings, in which like reference numerals represent like parts:

[0012] FIG. 1 illustrates a simplified block diagram of a communication system may be utilized according to an embodiment of the present disclosure;

[0013] FIG. 2 illustrates the interactions among components in a communication system for verifying a lead according to an embodiment of the present disclosure;

[0014] FIG. 3 illustrates a process in a lead generator for providing a lead that can be verified according to an embodiment of the present disclosure;

[0015] FIG. 4 illustrates a process in a verification server for supporting the lead verification service according to an embodiment of the present disclosure;

[0016] FIG. 5 illustrates an example of monitoring a web page that hosts the lead generator according to an embodiment of the present disclosure; and

[0017] FIG. 6 illustrates a system suitable for implementing one or more embodiments of the present disclosure.

DETAILED DESCRIPTION OF THE INVENTION

[0018] FIGS. 1 through 6, discussed below, and the various embodiments used to describe the principles of the present disclosure in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the disclosure. Those skilled in the art will understand that the principles of the present disclosure may be implemented in any suitably arranged system. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, the disclosed embodiments are provided such that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. The principles and features of this invention may be employed in varied and numerous embodiments without departing from the scope of the invention.

[0019] Furthermore, well known or widely used techniques, elements, structures, and processes may not be described or illustrated in detail to avoid obscuring the disclosure. Although the drawings represent embodiments of the disclosure, the drawings are not necessarily to scale and certain features may be exaggerated or omitted in order to better illustrate and explain the present invention.

[0020] Embodiments of the present disclosure assume that lead sellers will want to provide a certificate of authenticity with every lead. Doing so lends credibility as they are willing to have their leads independently verified by a third party. Embodiments of the present disclosure also assume that an unscrupulous lead vendor would want to trick a verification server into misreporting the URL of a page where a lead was collected. Without proper means of authentication these unscrupulous lead vendors would be free to misrepresent an Internet lead while maintaining the appearance of being a trustworthy vendor. Embodiments of the present disclosure take a passive approach to solving this problem by quietly monitoring attempts to circumvent the verification process. The verification server does not expose to the lead vendor which checks are being performed when generating a reference key (e.g. verification token) that can later be used by a lead buyer to verify the authenticity of the lead information. Instead, each reference key is used to register a list of “suspicions” that are internally monitored for malfeasance. Sus-

picious can be used to register a level of confidence that the information collected and associated with a reference key was legitimately generated.

[0021] FIG. 1 is a simplified block diagram illustrative of a communication system **100** that may be utilized by various embodiments of the disclosure. The communication system **100** includes a visitor **110**, a lead generator (e.g. lead seller) **120**, a verification server (also referred to as a “trust form server”) **130**, and at least one lead buyer **140**. The communication system **100** may be utilized to facilitate communication between the described elements **110-140** through a private communication network (such as a local area network (LAN)) or a public communication network such as the Internet in order to allow verification of a lead provided by the lead generator **120**. In other configurations, the communication system **100** may utilize any other suitable communication technology.

[0022] As used herein, each of the elements **110-140** may generally refer to any object, device, server, software, web page, or any combination of the preceding that is generally operable to communicate with another element. The elements **110-140** may also represent a user profile representing a person. The user profile may comprise, for example, an address for the user, a user name, a pass code, other user information, or any combination of the preceding. Additionally, the elements **110-140** may represent a device that comprises any hardware, software, firmware, or combination thereof operable to communicate through the communication system **100**.

[0023] The visitor **110** may be a user (e.g. a consumer) or a computing device (e.g. a personal computer, a laptop, a mobile device, and such) controlled by the user to communicate with the lead generator **120** and submit contact information (e.g. lead data).

[0024] The lead generator **120** may be a website, a software program, a service, a form or script embedded onto a web page, or a web server that hosts a web page through which the visitor **110** may submit lead data. Lead data may include, but is not limited to, contact information of a person or entity, the type of product or service that the person or entity is interested in purchasing, information related to pre-qualification to a purchase, purchase preferences, and any other information that may generally be gathered concerning the visitor **110**. The lead generator **120** may also refer to the hosting page that hosts a script for supporting the lead verification service. When the visitor accesses the web page that hosts the lead generator **120**, the lead generator **120** may be executed in the visitor's browser.

[0025] According to certain configurations, the lead generator **120** may embed a script onto a web page that contains a form (e.g. hosting page) for submitting lead information. The script may also be placed on any web page (including those that don't contain the form). The script may be written in any appropriate language (e.g. Perl, JavaScript, Ruby, Python, and such) and installed by the publisher of the hosting page or form. When the visitor **110** establishes a connection with the lead generator **120**, the lead generator **120** notifies the verification server **130**. According to an embodiment, a series of scripts may be loaded by a visitor's browser from the verification server, the verification server generates a certificate for every visit to a page. According to an embodiment, the notification may comprise a request for a reference key that can be used to verify the lead information submitted by the visitor **110**. Upon receiving the reference key from the

US 2012/0290491 A1

Nov. 15, 2012

3

verification server **130**, the lead generator **120** associates the lead information submitted by the visitor **110** with the reference key and sends the reference key along with the lead information to at least one lead buyer **140**.

[0026] In certain configurations, the lead generator **120** may determine the appropriate lead buyer **140** based on the lead information. For example, any one or more of the contact information, qualification attributes, type of product or service requested, and such, may be used to determine to which lead buyers **140** the lead information should be sent. In addition, the appropriate lead buyer(s) **140** may be selected based on any additional scheme. For example, the lead buyers may be notified of the newly submitted lead information and be given the opportunity to purchase the lead information. In other configurations, the lead generator **120** may simply send lead information to a pre-programmed destination. Furthermore, although FIG. 1 shows a direct communication between the lead generator **120** and the lead buyer **140**, in certain configurations, there may be intermediate elements between the two.

[0027] The verification server **130** performs operations related to storing information that may be used to verify the lead data collected by the lead generator **120**. In particular configurations, the verification server **130** collects information about the visitor **110** and the lead generator **120** during the communication session during which the lead generator **120** receives contact information and other relevant information (i.e. lead data) submitted by the visitor **110**.

[0028] The information collected by the verification server **130** may include, but is not limited to, the Uniform Resource Locator (URL) of the hosting page (where the script is located) and/or the form where the lead data is being collected, Hypertext Transfer Protocol (HTTP) headers for the web page (e.g. for the lead generator or User-Agent) from the visitor **110**'s browser, date and time that the visitor arrived at the hosting page or submitted the lead data, and the internet protocol (IP) address of the visitor **110**. Additionally, in particular configurations, the verification server **130** may capture a screenshot of the hosting page or the form being submitted by the visitor **110** and/or text associated with a form that may be populated by a visitor accessing a website for the form. For example, in particular configurations, the text may be associated with terms or conditions corresponding to a form. The collected information may be stored in a certificate that can later be retrieved by at least one lead buyer **140** to verify the authenticity or validity of the corresponding lead data purchased or acquired from the lead generator **120**.

[0029] In particular configurations, the verification server **130** may be a computer system that communicates with the lead generator **120** and at least one lead buyer **140**. When contacted by the lead generator **120**, the verification server **130** generates the reference key (e.g. a token) and sends the reference key to the lead generator **120**. The reference key may be included in a token and comprise a string of unique alphanumeric characters that becomes associated with the certificate (i.e. information collected by the verification server **130**) and the lead data collected by the lead generator **120**. This information together (lead data and reference key) may be communicated to a lead buyer **140**.

[0030] When the lead buyer **140** sends a request for the certificate along with the reference key, the verification server **130** sends information corresponding to the certificate or the certificate, itself, to the lead buyer **140**.

[0031] In particular configurations, the lead buyer **140** may be a product/service vendor, computer, or an online account that represents the vendor. According to an embodiment, the verification server **130** may only provide information corresponding to the certificate or the certificate, itself, to a lead buyer that subscribes to the verification service. In this configuration, the lead buyer **140** must be a subscriber of the verification service in order to receive the certificates from the verification server **130**. The certificate will include the information collected by the verification server **130** about the visitor **110** and the hosting page of the lead generator **120** during the submission of the lead data. According to the embodiment, the certificate may include one or more of the information described in Table 1.

TABLE 1

INFORMATION	DESCRIPTION
Page URL	where the lead was collected, and the URLs of any containing pages, in the event that inline frames (IFrames) are employed on the hosting page
HTTP Headers	from the browser of visitor 110 , regarding the lead generator
Date & Time	when the visitor 110 arrived at the hosting page to submit the lead information
IP address	of the visitor 110
Form information	Any information associated with a form filled out by a visitor, including the form displayed and the text associated with the form

[0032] In particular configurations, data may be collected by the verification server **130** and not sent to the lead buyer **140**. Rather, a subset of information may be sent.

[0033] According to certain configurations, the verification server **130** may ignore or actively avoid collecting any personally identifiable information about the visitor **110** in order to maintain privacy and integrity. Any personal information that may have been inadvertently collected may not be included in the certificate data that is sent to the requesting lead buyer **140**. For example, when capturing the page URL, where the lead is collected, it is possible that additional data is captured as additional parameters appended to the page URL. As the data appended to the page URL is at the discretion of the publisher of the hosting page, personal information that is appended to the URL (e.g. name of the lead or traffic data) may inadvertently be collected by the verification server **130**, which captures the complete URL. According to an embodiment, the verification server **130** may hide or remove the personal information that is appended to the captured URL of the hosting page for the lead generator **120**.

[0034] Because the script installed on the lead generator **120** only causes the verification server to be notified and to include the reference key (i.e. token) into the lead form, changes regarding the type of verification information that is collected to authenticate the lead generator **120** only need to be implemented by the verification server **130**. This allows the verification server to be flexible in modifying or enhancing verification techniques as lead vendors become savvier and HTML code becomes more advanced. As such, the entire process can be easily altered without requiring intervention or allowing interference from lead vendors. Put another way, the

US 2012/0290491 A1

Nov. 15, 2012

4

authentication process can be changed at any time without any coordination with the lead vendors who have chosen to implement the script.

[0035] FIG. 2 illustrates the interactions in a communication system for verifying a lead according to an embodiment of the disclosure. In block 210, the lead generator 120 detects that a visitor (e.g. visitor 110) has accessed the hosting page for submitting lead information. When the visitor accesses the host page of the form, the lead generator 120 (which is being executed in the visitor's browser) executes a script that was embedded in the form by the lead vendor to send a reference key request 220 to the verification server 130. The reference key request 220 may include information about the user-agent of the visitor browser, the visitor's IP address, a timestamp, and the URL of the form. In other configurations, the reference key request 220 may occur at any suitable time. In certain configurations, notifying the verification server 130 may constitute a request for a reference key.

[0036] Upon receiving the reference key request 220, the verification server 130 issues the reference key 230 to the lead generator 120. The verification server 130 may also begin to collect information about the visitor and/or the lead generator 120 in block 240. The collected information becomes associated with the reference key 230. As discussed above, in certain configurations, the collected information and the reference key 230 is stored as a certificate that can be identified by the reference key 230 on the verification server 130. In certain configurations, the verification server 130 may begin collecting the information in block 240 upon receiving the reference key request 220 and concurrently with or prior to issuing the reference key 230.

[0037] According to an embodiment, issuing the reference key 230 may comprise a two-step process to ensure that the scripts loaded from the verification server 130 are not altered. In a first step of the embodiment, the lead verification server 130 captures the relevant data from the reference key request 220 (e.g. information about the user-agent of the visitor browser, the visitor's IP address, a timestamp, and the URL of the form) as described with reference to block 240, stores the captured data into a document (e.g. certificate) and sends a script download token to visitor's browser that is executing the lead generator 120. The script download token (e.g. reference key) is embedded in a first script which is returned to and executed in the visitor's browser. The purpose of the first script returned to the visitor's browser in the first step is to request a second script which will insert the URL of the corresponding document stored in the verification server 130 into the form of the lead generator 120. The request for the second script contains the URL of the browser's document location and the "script download token" generated during the first step. If the lead generator 120 or a lead vendor tries to skip the first step, then the verification server 130 will record a suspicion in the document generated during the first. Suspicions will also be recorded if the IP addresses or user-agents of the first and second steps do not match, or if the script download token has already been used or cannot be found. In an embodiment, the script download token may self-destruct or be rendered useless after a predetermined time period (e.g. 120 seconds), thereby preventing a lead vendor from generating them in bulk for later use. In some embodiments multiple processes may also be used on consecutive requests as a way to confuse unscrupulous vendors. In this way, the verification server 130 may ensure that the scripts are being loaded directly from the verification server 130, thereby

thwarting an unscrupulous vendor that may try downloading the script, altering it, and then inserting the altered script into the lead generator 120 being run in the visitor's browser. This would also prevent the vendor from issuing reference keys or other false URLs of the verification certificate.

[0038] According to some embodiments, the verification server 130 may want to ensure that the scripts are being performed in the visitor's browser. By including a script that must be successfully executed, the verification server 130 may ensure that the script is being executed in an appropriate script interpreter, rather than just parsed as a string for pertinent information. For example, the verification server 130 may perform a calculation during the first step and ask the browser to perform the same calculation. The verification server 130 would check the visitor browser's calculation during the second step. If the calculations do not match, then a suspicion would be registered in the corresponding certificate. Obfuscation of the script code returned to the visitor's browser can be used to prevent simple parsing by the lead vendor's code. This would be most effective if the obfuscation techniques are rotated in random ways, making it difficult for the lead vendor's server-side code to fetch information out of the script without actually evaluating it in a script engine.

[0039] The verification server 130 may also count the number of certificates generated by requests from the same IP address. If a high number of certificates are being generated by the same IP address, then a suspicion would be recorded with the corresponding certificates. In another embodiment, certain script calls to a document object model in the hosting page can be used to ensure that the script interpreter executing the code is being run in a browser rather than in a stand-alone interpreter like Rhino or V8.

[0040] In particular configurations, the verification server 130 may also continue to monitor the hosting page of the lead generator 120 over time, thereafter. As mentioned previously, reference key 230 may be included in a token and comprise a string of unique alphanumeric characters. The verification server 130 may generate or assign the reference key 230.

[0041] In block 250, the lead generator 120 associates the received reference key 230 with the form that is being populated by the visitor for submission of lead information. According to certain configurations, the reference key 230 may be stored in a hidden field of the form. In the hidden field, the reference key 230 may also be included in a certificate URL that can be used to access the stored certificate on the verification server 130.

[0042] In block 260, the lead generator 120 detects that the visitor has completed the form and submitted the lead information. The lead generator 120 then sends the submitted form data 270 to at least one lead buyer 140 or alternatively to an intermediate element that may, in turn, submit the data to the lead buyer 140. The submitted form data 270 includes the lead information and the reference key 230.

[0043] The lead buyer 140 may then send a certificate request 280 to the verification server 130 to verify, among other things, the authenticity of the lead information that was included in the received form data 270. According to an embodiment, the lead buyer 140 may include the reference key 230 in the certificate request 280. Alternatively, if the certificate URL is included in the form data 270, the lead buyer 140 may attempt to access the certificate URL, which may be constituted as the certificate request 280.

[0044] Upon receiving the certificate request 280 (which includes the reference key 230), the verification server 130

US 2012/0290491 A1

Nov. 15, 2012

5

may retrieve the stored certificate based on the reference key **230** and send the certificate data **290** to the lead buyer **140**. In an embodiment, the verification server **130** may first determine whether the lead buyer **140** is a valid subscriber to the verification service before sending the certificate data **290**.

[0045] FIG. 3 illustrates a process **300** in a lead generator for providing a lead that can be verified according to an embodiment of the present disclosure. The lead generator may be any web page, form, or script on a hosting page where a visitor may submit their lead information, such as lead generator **120**.

[0046] In block **310**, the lead generator detects that a visitor has landed on the hosting page that contains the form for submitting lead information. In block **320**, the lead generator sends a request for a reference key to a verification server (e.g. the verification server **130**). In certain configurations, the lead generator simply notifies the verification server that a visitor has landed on the hosting page.

[0047] In block **330**, the reference key is received and assigned to the instance of the form that the visitor is using to submit the lead information. According to certain configurations, the reference key is stored in a hidden field on the form and may be included in a certificate URL.

[0048] In block **340**, the lead generator determines whether the form has been submitted. If the form is not submitted, the process **300** ends. According to an embodiment, the lead generator may determine that the form is not submitted if the form is not submitted within a specified period, the web browser is closed before the visitor submits the lead information, or the visitor navigates away from the hosting page without submitting the lead information.

[0049] In contrast, if the form is submitted, the lead generator sends the lead data to at least one lead buyer in block **360** (or alternatively to an intermediate element that is in communication with the lead buyer) and ends the process. According to certain configurations, the lead generator may determine to which lead buyer(s) the lead information is to be sent based on at least a portion of the lead information in the submitted form.

[0050] FIG. 4 illustrates a process **400** in a verification server for supporting the lead verification service according to an embodiment of the present disclosure. The verification server (e.g. the verification server **130**) may be a computer system that communicates with at least one lead generator (e.g. the lead generator **120**) and at least one lead buyer (e.g. the lead buyer **140**).

[0051] In block **410**, the verification server receives a request for a reference key from a lead generator. As described earlier, the request may simply be a notification that a visitor has landed on a hosting page of the lead generator. In block **420**, a reference key is generated and sent to the requesting lead generator. In an embodiment, the verification server may generate a token that serves as the reference key and send the token to the lead generator.

[0052] In block **430**, the verification server begins to collect information about the visitor the hosting page of the lead generator that requested the reference key. The information collected by the verification server may include, but is not limited to, the Uniform Resource Locator (URL) of the hosting page or form where the lead data is being collected, Hypertext Transfer Protocol (HTTP) headers for the web page (e.g. for the lead generator or User-Agent) from the visitor's browser, date and time that the visitor arrived at the hosting page or submitted the lead data, and the internet

protocol (IP) address of the visitor. Additionally, the verification server may capture a screenshot of the hosting page or the form being submitted by the visitor and/or text associated with a form that may be populated by the visitor accessing a website for the form. For example, in particular configurations, the text may be associated with terms or conditions corresponding to a form. The collected information may be stored in a certificate or some other data structure that can be identified by the reference key. In certain configurations, the verification server may continue to monitor the hosting page of the lead generator over time and, as appropriate, provide such monitored information to a lead buyer. Additionally, according to certain configurations, the verification server may take affirmative steps to not collect any personally identifiable information about the visitor or traffic data and/or may remove such personally identifiable information.

[0053] In block **440**, a request for certificate data is received. The request may be transmitted from a lead buyer that purchased or acquired lead information that included the reference key.

[0054] In block **450**, the certificate data that corresponds to the reference key included in the request is transmitted to the lead buyer that sent the request. That is, the verification server determines the reference key from the request for certificate data, retrieves the corresponding certificate data (or data structure) based on the reference key, and sends the retrieved certificate data to the lead buyer. In particular configurations, monitored information may additionally be communicated to the lead buyer.

[0055] According to certain configurations, the verification server may first determine whether the lead buyer is a subscriber of the verification service or has appropriate access to the certificate data before sending the certificate data. For example, the verification server may request a password, or the request for certificate data may include authentication information that identifies the lead buyer. If the requesting lead buyer does not have access, the verification server may not send the requested certificate data.

[0056] According to certain configurations, as alluded to above, the verification server may also check the certificate data to ensure that personal information of the visitor or traffic information that reveals the referrer of the lead generator is not sent with the certificate data.

[0057] FIG. 5 illustrates an example of monitoring a web page that hosts the lead generator according to an embodiment of the present disclosure. Web page **610** is hosted on a lead vendor's server. The web page **610** contains a form **614** and a script **618** that has been added by the lead vendor. When executed by a visitor's browser, the script **618** on the web page **610** (e.g. lead generator **120**) communicates with the verification server **130**. In a request for a reference key, the script **618** provides to the verification server **130** the URL **620** of the web page **610** where the form **614** resides. At this point, the verification server **130** is "aware" of the URL of the form **614** and begins to monitor the web page **610** for any changes. The changes to the web page **610** may be presented in an event timeline as shown in sample snapshots **630-650**. The first snapshot **630** of the web page **610** may be taken when the verification server first receives a notification (or reference key request) from the script **618**. From there on, the verification server **130** monitors the web page **610**. The second and third snapshots **640** and **650** are taken when the changes are detected by the verification server **130**. According to an embodiment, for each change detected, snapshots of the web

US 2012/0290491 A1

Nov. 15, 2012

6

page 610 are captured including at least one of the HTML, image files, and a high-resolution, full-length image of the web page 610.

[0058] FIG. 6 illustrates a system suitable for implementing one or more embodiments of the present disclosure. System 500 may be used in connection with other embodiments of the disclosure to carry out any of the above-referenced functions and/or serve as a computing device for performing the functions of the lead generator 120 and/or the verification server 130 of FIG. 1. The computer system 500 includes a processor 502 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 508, read only memory (ROM) 510, random access memory (RAM) 512, input/output (I/O) device 506, and network connectivity devices 504. The processor 502 may be implemented as one or more CPU chips.

[0059] The secondary storage 508 typically includes one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM 512 is not large enough to hold all working data. Secondary storage 508 may be used to store programs that are loaded into RAM 512 when such programs are selected for execution. Secondary storage devices 508 may include a variety of types of storage media such as, for example, floppy disk drives, hard disk drives, CD ROM drives, DVD ROM drives, magnetic tape drives, solid state devices, or other suitable storage media. Although this embodiment employs a plurality of disk drives 508, a single disk drive 508 may be used without departing from the scope of the disclosure. The ROM 510 is used to store instructions and perhaps data that are read during program execution. ROM 510 is a non-volatile memory device that typically has a small memory capacity relative to the larger memory capacity of secondary storage. The RAM 512 is used to store volatile data and perhaps to store instructions. Access to both ROM 510 and RAM 512 is typically faster than to secondary storage 508.

[0060] I/O devices 506 may include printers, video monitors, liquid crystal displays (LCDs), touch screen displays, keyboards, keypads, switches, dials, mice, track balls, voice recognizers, card readers, paper tape readers, or other well-known input devices. The network connectivity devices 504 may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area network (WLAN) cards, radio transceiver cards such as code division multiple access (CDMA) and/or global system for mobile communications (GSM) radio transceiver cards, and other well-known network devices. The network devices 504 may be connected to a computer network or a variety of other communicative platforms including, but not limited to, a public or private data network; a local area network (LAN); a metropolitan area network (MAN); a wide area network (WAN); a wire line or wireless network; a local, regional, or global communication network; an optical network; a satellite network; an enterprise intranet; other suitable communication links; or any combination of the preceding. These network connectivity devices 504 may enable the processor 502 to communicate with an Internet or one or more intranets. With such a network connection, it is contemplated that the processor 502 might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Such information, which is often represented

as a sequence of instructions to be executed using processor 502, may be received from and outputted to the network, for example, in the form of a computer data signal embodied in a carrier wave.

[0061] Such information, which may include data or instructions to be executed using processor 502 for example, may be received from and outputted to the network, for example, in the form of a computer data baseband signal or signal embodied in a carrier wave. The baseband signal or signal embodied in the carrier wave generated by the network connectivity devices 504 may propagate in or on the surface of electrical conductors, in coaxial cables, in waveguides, in optical media, for example optical fiber, or in the air or free space. The information contained in the baseband signal or signal embedded in the carrier wave may be ordered according to different sequences, as may be desirable for either processing or generating the information or transmitting or receiving the information. The baseband signal or signal embedded in the carrier wave, or other types of signals currently used or hereafter developed, referred to herein as the transmission medium, may be generated according to several methods well known to one skilled in the art.

[0062] The processor 502 executes instructions, codes, computer programs, scripts, as such, for performing the processes discussed in the present disclosure. The instructions, codes, computer programs, or scripts may be accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage 508), ROM 510, RAM 512, or the network connectivity devices 504.

[0063] Although FIG. 6 provides one embodiment of a computer system that may be utilized with other embodiments of the disclosure, such other embodiments may additionally utilize computers other than general purpose computers as well as general purpose computers without conventional operating systems. Additionally, embodiments of the disclosure may also employ multiple computer systems 500 or other computers networked together in a computer network. Most commonly, multiple general purpose computers 500 or other computers may be networked through the Internet and/or in a client server network. Embodiments of the disclosure may also be used with a combination of separate computer networks each linked together by a private or a public network.

[0064] Several embodiments of the disclosure may include logic contained within a non-transitory storage medium. In the embodiment of FIG. 6, the logic includes computer software executable on the system 500. The medium may include the RAM 512, the ROM 510, the disk drives 508, or other mediums. In other embodiments, the logic may be contained within hardware configuration or a combination of software and hardware configurations.

[0065] The logic may also be embedded within any other suitable medium without departing from the scope of the disclosure.

[0066] It will be understood that well known processes have not been described in detail and have been omitted for brevity. Although specific steps, structures and materials may have been described, the present disclosure may not be limited to these specifics, and others may be substituted as it is well understood by those skilled in the art, and various steps may not necessarily be performed in the sequences shown.

[0067] While several embodiments have been provided in the present disclosure, it should be understood that the disclosed systems and methods might be embodied in many

US 2012/0290491 A1

Nov. 15, 2012

7

other specific forms without departing from the spirit or scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details given herein. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted, or not implemented.

[0068] Also, techniques, systems, subsystems and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other products shown or discussed as directly coupled or communicating with each other may be coupled through some interface or device, such that the products may no longer be considered directly coupled to each other but may still be indirectly coupled and in communication, whether electrically, mechanically, or otherwise with one another. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

What is claimed is:

1. A method of providing a lead that can be verified, the method comprising:

notifying a verification server when a visitor accesses a web page to enter information into a form;
receiving a reference key comprising a unique identifier from the verification server; and
in response to the visitor submitting the form, sending the form data to at least one interested party, the form data comprising the reference key and at least some of the information entered into the form.

2. The method of claim 1, further comprising storing the reference key in the form, wherein the reference key allows the at least one interested party to verify the form data.

3. The method of claim 2, wherein storing the received reference key in the form comprises:

storing a verification universal resource locator (URL) that includes the reference key.

4. The method of claim 3, wherein receiving a reference key comprising a unique identifier from the verification server comprises:

receiving a script comprising the reference key;
sending a request for a verification universal resource locator (URL) according to the script, the request comprising the reference key;
receiving the verification URL, the verification URL comprising the reference key; and
storing the verification URL in the form data.

5. The method of claim 1, wherein the information entered by the visitor comprises at least one of contact information, a product description, and a service description.

6. A method for supporting a lead verification service, the method comprising:

in response to receiving a notification from a lead generator on a website that is being accessed by a visitor, generating a reference key comprising a unique identifier;
sending the reference key to the lead generator;
collecting information about the lead generator and the visitor that is accessing the website, the collected information associated with the reference key; and
sending at least some of the collected information to an interested party in response to receiving a valid request comprising the reference key.

7. The method of claim 6, wherein the collected information comprises at least one of a universal resource locator (URL) of the website for the lead generator, at least one header of the website, a date and a time that the visitor is accessing the website, and an Internet protocol (IP) address of the visitor.

8. The method of claim 6, wherein sending the at least some of the collected information to the interested party in response to receiving a valid request comprises retrieving the collected information based on the reference key included in the request.

9. The method of claim 8, wherein sending the at least some of the collected information to the interested party in response to receiving a valid request further comprises:

determining whether the interested party is a valid subscriber of the verification service; and
in response to determining that the interested party is a valid subscriber, sending the at least some of the collected information to the interested party.

10. The method of claim 6, wherein sending the reference key to the lead generator comprises:

sending a script comprising the reference key;
receiving a request for a verification universal resource locator (URL), the request comprising the reference key;
determining whether the script was executed on the visitor's computer;
in response to determining that the script was not executed on the visitor's computer, recording a suspicion along with the collected information; and
sending the verification URL to the lead generator.

11. A system for supporting a lead verification service, the system comprising:

a verification server; and
a web server that is hosting a website comprising a lead generator, the lead generator configured to:
notify the verification server when a visitor accesses the website to enter information into a form,
receive a reference key comprising a unique identifier from the verification server, and
send the form data to at least one interested party in response to the visitor submitting the form, the form data comprising the reference key and the information entered by the visitor.

12. The system of claim 11, wherein the instance of the lead generator is further configured to store the reference key in the form, wherein the reference key allows the at least one interested party to verify the form data.

13. The system of claim 11, wherein when storing the received reference key in the form, the instance of the lead generator is further configured to generate a verification universal resource locator (URL) that includes the reference key.

14. The system of claim 11, wherein when receiving a reference key comprising a unique identifier from the verification server, the lead generator is further configured to:

receive a script comprising the reference key;
send a request for a verification universal resource locator (URL) according to the script, the request comprising the reference key;
receiving the verification URL that comprises the reference key; and
storing the verification URL in the form data.

15. The system of claim 11, wherein the information entered by the visitor comprises at least one of contact information, a product description, and a service description

US 2012/0290491 A1

Nov. 15, 2012

8

16. An apparatus for supporting a lead verification service, the apparatus comprising:

a communication interface configured to send and receive information;

a memory configured to store instructions for providing lead information that can be verified; and

a processor configured to perform the instructions stored in the memory, the instructions configured to:

generate a reference key comprising a unique identifier in response to receiving a notification from a lead generator on a website that is being accessed by a visitor,

send the reference key to the lead generator,

collect information about the lead generator and the visitor that is accessing the website, the collected information associated with the reference key, and

send at least some of the collected information to an interested party in response to receiving a valid request comprising the reference key.

17. The apparatus of claim **16**, wherein the collected information comprises at least one of a universal resource locator (URL) of the website for the lead generator, at least one header of the website, a date and a time that the visitor is accessing the website, and an internet protocol (IP) address of the visitor.

18. The apparatus of claim **16**, wherein sending the at least some of the collected information to the interested party in response to receiving a valid request further includes retrieving the collected information based on the reference key included in the request.

19. The apparatus of claim **18**, wherein sending the at least some of the collected information to the interested party in response to receiving a valid request further includes:

determining whether the interested party is a valid subscriber of the verification service; and

sending the collected information to the interested party in response to determining that the interested party is a valid subscriber.

20. The apparatus of claim **16**, wherein when sending the reference key to the lead generator, the verification server is further configured to:

send a script comprising the reference key;

receive a request for a verification universal resource locator (URL), the request comprising the reference key;

determine whether the script was executed on the visitor's computer;

in response to determining that the script was not executed on the visitor's computer, record a suspicion along with the collected information; and

send the verification URL to the lead generator.

* * * * *